AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

356 HILLWOOD COURT,
HERNDON, VIRGINIA 20170

Case No. 1:17-SW- 605

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, which is incorporated by reference

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 875(c)	Interstate Communication of Threats

The application is based on these facts:

See attached Affidavit, which is incorporated by reference

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Sarah Thaden
Applicant's signature

Sarah Thaden, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 09/16/2017

Judge's signature

City and state: Arlington, Virginia

The Honorable Michael S. Nachmanoff
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is 356 HILLWOOD COURT, HERNDON, VIRGINIA 20170, as well as any vehicles, outbuildings, storage lockers (including safes) and electronic media (*e.g.*, computers, wireless telephones, and other storage media, such as scanners, external storage media, and printers with memory capability) located thereon. The subject residence is a two-story, single-family home with the following features: brick on the lower half of the house; white coloring on the top half; a brown front door; and a two-car attached garage. The house number "356" appears on the mailbox in front of the residence.

ATTACHMENT B

Property to be seized

1. All records relating to violations of Title 18, U.S. Code, Section 875(c), those violations involving WILLIAM LEWIS WEAVER, II and occurring on or after February 15, 2016, including:

a. Records and information relating to communications transmitted in interstate commerce that contain threats to injure the person of another, including federal officials or employees, federal law enforcement officers, or local law enforcement officers;

b. Records and information relating to WEAVER's use of, and access to, Twitter, including the use or access of the Twitter account @WillWeaver2;

c. Records and information relating to the e-mail account will.w@truehitdesigns.com;

d. Records and information relating to the identity or location of WEAVER;

e. Records and information relating to communications with Internet Protocol addresses 108.45.77.58; 191.238.8.154; 191.238.9.94; 191.238.9.80; 208.54.35.182; 64.121.165.36;

f. Records and information referring or relating to identities or aliases of WEAVER;

g. Records and information referring or relating to past travel or planned travel by WEAVER, including airline tickets, credit card bills, bank records, checks, itineraries, passports, and visas;

h. Records and information relating to accounts with any Internet service provider that is assigned to or controlled by WEAVER;

i. Records and information referring or relating to any storage facilities, safety deposit boxes, mailboxes, or other locations where any of the foregoing items may be located;

j. Any and all firearms, ammunition, body armor, military-style equipment, knives, swords, explosive materials or their precursors, or other weapons;

k. Records and information referring or relating to the purchase of firearms, body armor, military-style equipment, knives, swords, explosive materials or their precursors, or other weapons;

l. Records and information referring or relating to the building of explosive materials, including periodicals, magazines, books, or articles;

2. Computers or storage media used as a means to commit the violations described above, including transmitting, in interstate commerce, communications that contain threats to injure the person of another, in violation of 18 U.S.C. § 875(c).

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF 356 HILLWOOD COURT, HERNDON, VIRGINIA 20170	Case No. 1:17-SW- 605 **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Sarah Thaden, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 356 HILLWOOD COURT, HERNDON, VIRGINIA 20170 (hereinafter, "**SUBJECT PREMISES**"), which is owned by WILLIAM LEWIS WEAVER, II, and is further described in Attachment A, for the things described in Attachment B.

2. Your Affiant is a Special Agent with the Federal Bureau of Investigation ("FBI") and has been so employed since approximately March 2016. I am assigned to the Washington Field Office, Northern Virginia Violent Crimes Task Force. Prior to being hired as a Special Agent with the FBI, I was a police officer with the Charlottesville Police Department and was so employed from approximately July 2011 to February 2016.

3. I am a graduate of the FBI Basic Field Training Course in Quantico, Virginia, and the Basic Law Enforcement Training Course at the Central Shenandoah Criminal Justice Training Academy in Weyers Cave, Virginia. I have received formal training in the investigation of violent crimes, including specialized training in forensic evidence collection. I

have received training regarding computer crimes and have participated in the execution of search warrants involving electronic evidence. I have a graduate degree in Linguistics, focusing on Forensic and Sociolinguistics. I have investigated or assisted in the investigation of a number of cases involving violent criminal activity and crimes against persons and property. I have been a sworn law enforcement officer during all times herein.

4. The facts and information contained in this Affidavit are based upon my training and experience, participation in federal investigations, personal knowledge, and observations during the course of this investigation, as well as the observations of other agents involved in this investigation. All observations not personally made by me were related to me by the individuals who made them or were conveyed to me by my review of records, documents, and other physical evidence obtained during the course of this investigation. This Affidavit contains information necessary to support probable cause and is not intended to include each and every fact and matter observed by me or known to the Government.

RELEVANT STATUTE

5. Based on my training and experience, and discussions with federal prosecutors assigned to this investigation, I have learned that Title 18, U.S. Code, Section 875(c) makes it a crime to transmit, in interstate commerce, communications which contained threats to injure the person of another.

TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

7. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state or country.

8. An "Internet Protocol address," or "IP address," is a unique numeric address used to identify computers or other electronic devices on the Internet. The standard format for IP addresses consists of four numbers between 0 and 255 separated by dots, *e.g.*, 149.101.10.40. Every computer or other electronic device connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to a particular computer or other electronic device, is directed properly from its source to its destination.

9. "Emails" sent over the Internet contain records of IP addresses that can be used to determine the origin and destination of the message. The "header" of an email, which is attached to the top of every email and contains IP addresses of computers or other electronic devices that have transmitted the email, may be used to identify the "path" through the Internet the email traveled from its origin to its destination. The header will often contain the IP addresses of any and all servers from which the given email "bounced" en route to its destination. These IP addresses may be traced to determine the sender of a specific email.

10. A "wireless telephone," or "mobile telephone" or "cellular telephone," is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records at least the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include Global Positioning System ("GPS") technology for determining the location of the device, and may record GPS data.

11. A "digital camera" is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

12. A "portable media player," or "MP3 Player" or "iPod," is a handheld digital

storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

13. A "Global Positioning System navigation device" uses GPS technology to display its current location. It often records the locations where it has been. Some GPS navigation devices (or capabilities within a wireless telephone) can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

14. A "personal digital assistant," or "PDA," is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet

and send and receive email. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

15. A "tablet" is a mobile computer, such as an iPad, that is typically larger than a phone yet smaller than a notebook and is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving email, and participating in Internet social networks.

16. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

PROBABLE CAUSE

A. The SUBJECT PREMISES

17. The **SUBJECT PREMISES** includes the residence located at 356 HILLWOOD COURT, HERNDON, VIRGINIA 20170, which is within the Eastern District of Virginia.

18. As described below, Internet Protocol ("IP") address 108.45.77.58 has been traced to the **SUBJECT PREMISES** in connection with the use of the Twitter account @WillWeaver2 on or about September 14 and 15, 2017. Records obtained from Twitter and Verizon indicate that 108.45.77.58 is a Verizon Internet Services IP address, and that registered address for the subscriber of the associated Verizon Internet Services account is the **SUBJECT PREMISES**. Additionally, the **SUBJECT PREMISES** was listed by WEAVER as his address on the paperwork, including the customer order form, during WEAVER's attempted purchase of a firearm and ammunition on or about September 15, 2017, from a store located in Sterling, Virginia.

B. The Investigation of WEAVER

19. According to information received from City of Herndon Police Department, law enforcement officers have visited WEAVER at his residence in Herndon, Virginia, which is within the Eastern District of Virginia, on at least two occasions prior to September 14, 2017, as a result of postings on Twitter (or "tweets") associated with the Twitter handle @WillWeaver2. A review of @WillWeaver2's Twitter page, which is publically accessible, indicates that the account is based in "NOVA in VA." The Twitter page provides a link to a website with the domain name "william-weaver.com."

20. Information received from CIA's police department,[1] which has law enforcement authority with respect to its facilities, indicate that on or before June 17, 2017, @WillWeaver2 posted at least one tweet that was directed at the CIA and the National Security Agency. The communication(s) was/were concerning in nature and resulted in the City of Herndon Police Department conducting a welfare check of WEAVER at the **SUBJECT PREMISES**. During this meeting, WEAVER did not deny that he owns or controls @WillWeaver2, indicated that he had been intoxicated when he posted the tweet(s) in question, and did not intend to hurt anyone unless they came to his house.

21. According to the U.S. Department of State, on or about February 15, 2016, WEAVER submitted a passport application to the State Department. Then, approximately a year later, on or about February 6, 2017, WEAVER submitted another passport application to the State Department. The State Department has indicated that both applications were denied.

22. A review of the tweets posted on @WillWeaver2's Twitter page indicate that on or about August 29, 2017, @WillWeaver2 posted the following tweet regarding the CIA: "Logic continues to dictate that bombing the cia , and shotgunning them as they lineup outside the gate at work in the morn is my conclusion." Later on the same day, @WillWeaver2 posted another

---

[1] In a federal arrest warrant applied for and obtained on September, 15, 2017, from this Court within the Eastern District of Virginia, your Affiant indicated that this information was based on "records" received from CIA's police department. This description was erroneous; the information was communicated orally by CIA's police department to a law enforcement colleague of your Affiant's, who then relayed it to your Affiant.

tweet that, given its context, also appeared to concern the CIA: "They all line up at those gates like ducks at the county fair shooting gallery, haha.All that evil just a few shotgun blasts away from gone."

23. Also, I have seen a tweet by @WillWeaver2 that was posted on or about August 29, 2017, and appears to have been directed at the State Department. It read as follows: "@StateDept You have about 2 weeks 2 get my passport 2 me before the devices set off and the shotgun blasts start. Tick-tock goes the clock." I know that @StateDept is the official Twitter account handle for the U.S. State Department.

24. On or about September 14, 2017, law enforcement officers with the City of Herndon Police Department and FBI Task Force Officers, one of whom is a Diplomatic Security Special Agent for the Department of State, made contact with WEAVER at the **SUBJECT PREMISES**. The purpose of the contact was to explain to WEAVER that the prior issue with his application for a passport was believed to have been resolved and he could attempt to apply again. During this meeting, WEAVER was made aware that the Task Force Officer who was present at the door of the residence was a federal agent. WEAVER made several statements of note during this encounter, including the following: something to the effect of "[I]t's almost there. You are going to see;" "we are passed the courts;" and "I am on a set schedule for some events coming up that your folks should know about. I'm not who I once was."

25. My review of @WillWeaver2 indicates that, on or about September 15, 2017, @WillWeaver2, whose location is listed as "NOVA in VA," posted the following posts:

a. "Police rolled up on my house at 9:30pm, banging on my door. Another @StateDept clown w/ them, but they seemed to have forgotten my passport."

b. "Talking about how I could pay them and shit all over again for my passport. Talking lies in front of the officer, again. Fake ass warrants."

c. "Now I warned you cocksucking assbags @StateDept to get me my shit that's owned to me, yet you insult me by trying to strongarm me."

d. "A reminder: To anyone who attempts to disarm me, or detain me, I will attempt to kill w/ all that is me and any of your nearby associates."

e. "So the cops roll up on my pad trying to intimidate me, and failed. So I just rolled up on their HQ and told them to back the fuck off."

26. According to City of Herndon Police Department, on or about September 15, 2017, WEAVER appeared in person at the City of Herndon Police Department and said something to the effect that he did not have any issues with them.

27. My review of @WillWeaver2 indicates that on or about September 15, 2017 the following tweets were posted:

a. "I don't care if you're cia, nsa, police, military, nutty christians. If u fuck with me,I will find you and skull fuck each & every 1 of you."

b. "And to clarify, when the police came over to start shot, they were antagonizing, flashlight in my eyes, making threats. I didn't back down."

c. "Today's going to be real interesting. I'm charged up, and have a lot of work to get to. Do not come to my house unless you're looking to die."

d. "It might be best to assume that all are enemies at this point."

28. Based on information received from a store located in Sterling, Virginia, which is within the Eastern District of Virginia, WEAVER went to the store in person on or about September 15, 2017, and attempted to purchase a shotgun and ammunition. WEAVER reportedly paid for the weapon and ammunition at that time but was told by employees that he was unable to take the weapon or ammunition home immediately. During this attempted transaction, WEAVER completed paperwork relating to the purchase of the shotgun and ammunition, including a customer order form, in which he listed he **SUBJECT PREMISES** was as his address. WEAVER reportedly advised that he would return on or about September 16, 2017, to retrieve the weapon and ammunition.

29. My review of @WillWeaver2 indicates on or about September 15, 2017, the following tweets were posted:

a. "I tried to buy a shotgun for home defence. VA state police put it on delay. Can't trust police anymore. If denied Will get another way."

b. "Talking to other nations to help me escape this now hellhole. We'll see, need gun first for prorection."

30. Based on my training and experience, I know that tweets are posted on Twitter via an electronic device, such as a cellular telephone or computer, with an Internet connection. Based on information received from a representative of Twitter, I know that a tweet must be routed through one or more of Twitter's computer servers in order to be posted and that all of Twitter's computer servers are located outside of the state of Virginia. Accordingly, I submit

there is reason to believe that the tweets identified above were transmitted in interstate commerce.

C. Additional Facts Supporting Probable Cause to Search the SUBJECT PREMISES

31. Based on Twitter posts from @WillWeaver2 that include references to shotguns, shooting, and gathering in public places while "heavily armed", and on WEAVER's attempted purchase of a shotgun and ammunition on or about September 15, 2017, there is probable cause to believe there may be weapons, specifically firearms, in the **SUBJECT PREMISES**. In my training and experience, I know that individuals who possess weapons often store those weapons in their homes or vehicles for easy access and safe-keeping.

32. In addition, I have seen at least two tweets posted by @WillWeaver2 that reference the building or use of explosives. One such tweet, for instance, was the posting on or about August 29, 2017, which read as follows: "@StateDept You have about 2 weeks 2 get my passport 2 me before the devices set off and the shotgun blasts start. Tick-tock goes the clock." Another tweet that I have seen posted by @WillWeaver2 included a link to a PasteBin page, a popular website for storing and sharing text, on which there was a lengthy narrative. The narrative includes information indicating that WEAVER was the author of the narrative, and the narrative claims that WEAVER has attempted to build explosives in years past and has received training on building explosives.

33. Records obtained from Twitter indicate that @WillWeaver2 was created using email address will.w@truehitdesigns.com, and the mobile device associated with the Twitter account has a telephone number of 484-767-1610. According to the paperwork WEAVER

completed during his attempted purchase of a firearm on or about September 15, 2017, this telephone number is WEAVER's. Records from Twitter also indicate that several IP addresses have been used to log into @WillWeaver2, including: 191.238.8.154; 191.238.9.94; 191.238.9.80; 208.54.35.182; and 64.121.165.36. Law enforcement used an open source tool to determine that 108.45.77.58, which was used to log in to @WillWeaver2 on or about September 14 and 15, 2017, traced to Verizon Internet Services. Records obtained from Verizon indicate that 108.45.77.58 is associated with a subscriber named "Willaim Weaver" and the **SUBJECT PREMISES**.

34. Based on my training and experience, a person posting messages to Twitter while using an IP address that returns to a residence must necessarily use a computer or mobile device, such as a tablet or wireless telephone, to make those posts. It is therefore, reasonable to believe that computers, tablets, wireless telephones, and other electronic storage media may be present in the **SUBJECT PREMISES**.

COMPUTERS, TABLETS, WIRELESS TELEPHONES, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

35. As described within this Affidavit and in Attachment B, this application seeks permission to search for records that might be found on the **SUBJECT PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, tablet, wireless telephone, or other electronic storage media. Thus, the warrant applied for would authorize the seizure of computers, tablets, wireless telephones, and

other electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

36. *Probable cause.* For the reasons stated above, I submit there is probable cause to believe that computers, tablets, wireless telephones, or other electronic storage media will be found at the **SUBJECT PREMISES** that were used in furtherance of the criminal offenses described herein, or contain information relating to the criminal offenses described herein. If computers, tablets, wireless telephones, or other electronic storage media are, in fact, found on the **SUBJECT PREMISES**, there is probable cause to believe the records covered by this warrant will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that wireless telephones have capabilities that allow them to serve as: telephones, as described above in Paragraph 10; digital cameras, as described above in Paragraph 11; portable media players, as described above in Paragraph 12; GPS navigation devices, as described above in Paragraph 13; and PDAs, as described above in Paragraph 14. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

b. Further, based on my knowledge, training, and experience, I know that electronic devices—like computers, tablets, wireless telephones, and other electronic storage media—can store information for long periods of time on the devices. This information sometimes can be recovered with forensic tools.

c. In addition, based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a computer, tablet, wireless telephone, or other electronic storage media can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on computers, tablets, wireless telephones, or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a devices' operating system may also keep a record of deleted data in a "swap" or "recovery" file.

e. Wholly apart from user-generated files, electronic devices—in particular, computers' internal hard drives—contain electronic evidence of how the device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Electronic

device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

f. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

37. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer, tablet, wireless telephone, or other electronic storage media in the **SUBJECT PREMISES** because:

a. Data on such devices can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information

about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic devices may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such

information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how an electronic device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses an electronic device to post tweets that threaten another person, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The device is an instrumentality of the crime because it is

used as a means of committing the criminal offense. The device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a device used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

38. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing computers, tablets, wireless telephones, or other electronic storage media from the premises, it is sometimes possible to make an image copy of the computers, tablets, wireless telephones, or other electronic storage media. Generally speaking, imaging is the taking of a complete electronic picture of a device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic

electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Electronic devices, such as computers, can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the **SUBJECT PREMISES**. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the

warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

40. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES, as described in Attachment A, and to seize the items described in Attachment B.

Respectfully submitted,
/s/
Sarah Thaden, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on September 16, 2017:

The Honorable Michael S. Nachmanoff
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 356 HILLWOOD COURT, HERNDON, VIRGINIA 20170, as well as any vehicles, outbuildings, storage lockers (including safes) and electronic media (*e.g.*, computers, wireless telephones, and other storage media, such as scanners, external storage media, and printers with memory capability) located thereon. The subject residence is a two-story, single-family home with the following features: brick on the lower half of the house; white coloring on the top half; a brown front door; and a two-car attached garage. The house number "356" appears on the mailbox in front of the residence.

ATTACHMENT B

Property to be seized

1. All records relating to violations of Title 18, U.S. Code, Section 875(c), those violations involving WILLIAM LEWIS WEAVER, II and occurring on or after February 15, 2016, including:

a. Records and information relating to communications transmitted in interstate commerce that contain threats to injure the person of another, including federal officials or employees, federal law enforcement officers, or local law enforcement officers;

b. Records and information relating to WEAVER's use of, and access to, Twitter, including the use or access of the Twitter account @WillWeaver2;

c. Records and information relating to the e-mail account will.w@truehitdesigns.com;

d. Records and information relating to the identity or location of WEAVER;

e. Records and information relating to communications with Internet Protocol addresses 108.45.77.58; 191.238.8.154; 191.238.9.94; 191.238.9.80; 208.54.35.182; 64.121.165.36;

f. Records and information referring or relating to identities or aliases of WEAVER;

g. Records and information referring or relating to past travel or planned travel by WEAVER, including airline tickets, credit card bills, bank records, checks, itineraries, passports, and visas;

h. Records and information relating to accounts with any Internet service provider that is assigned to or controlled by WEAVER;

i. Records and information referring or relating to any storage facilities, safety deposit boxes, mailboxes, or other locations where any of the foregoing items may be located;

j. Any and all firearms, ammunition, body armor, military-style equipment, knives, swords, explosive materials or their precursors, or other weapons;

k. Records and information referring or relating to the purchase of firearms, body armor, military-style equipment, knives, swords, explosive materials or their precursors, or other weapons;

l. Records and information referring or relating to the building of explosive materials, including periodicals, magazines, books, or articles;

2. Computers or storage media used as a means to commit the violations described above, including transmitting, in interstate commerce, communications that contain threats to injure the person of another, in violation of 18 U.S.C. § 875(c).

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.